

Online Privacy and Personal Data Protection: An Islamic Law Perspective*

Bareq Muntadher Abdul Wahab¹, Safinaz Mohd Hussein²,
Ramalinggam Rajamanickam³

^{1,2,3} Universiti Kebangsaan Malaysia



[10.15408/jch.v13i3.46859](https://doi.org/10.15408/jch.v13i3.46859)

Abstract

This article explores the intricate intersection of online privacy and personal data protection through the lens of Islamic law, shedding light on the ethical considerations that govern digital transactions. Grounded in Qur'anic principles, Sunnah, and classical Islamic jurisprudence, this study examines how Shari'ah law provides a comprehensive ethical framework for navigating the digital landscape while upholding timeless Islamic values. Key principles such as Ghibah (gossip and backbiting), Amanah (trustworthiness), and Sitr (respect for privacy) are analyzed to highlight their significance in regulating online interactions and data protection. Employing a doctrinal legal method and an inductive approach, the article explores online privacy from an Islamic perspective. It incorporates Qiyas (analogical reasoning) to address emerging challenges posed by rapid technological advancements. The study finds that the commitment to Amanah underscores the responsibility of individuals, organizations, and governments in safeguarding personal information. It emphasizes ethical considerations in the collection, processing, and usage of data, aligning digital practices with Islamic moral obligations. Moreover, the dynamic nature of Ijtihad (independent legal reasoning) allows Islamic jurisprudence to adapt to contemporary digital issues while preserving its foundational ethical principles. By synthesizing Islamic teachings with digital ethics, this article offers a robust framework for addressing modern privacy concerns. It contributes to the discourse on the harmonious coexistence of technological innovations and Islamic values, providing insights into how Shari'ah law can guide ethical digital conduct. Ultimately, this study reinforces the relevance of Islamic legal principles in shaping responsible and morally sound digital practices.

Keywords: Online Privacy; Personal Data Protection; Islamic Principles; GDPR; CCPA

* Received: June 27, 2025, revised: July 26, 2025, accepted: July 29, 2025, published: December 30, 2025.

¹ Bareq Muntadher Abdul Wahab. PhD Student, Faculty of Law, Universiti Kebangsaan Malaysia. Email: bareq_montder@yahoo.com ORCID: <https://orcid.org/0009-0006-0989-6909>

² Safinaz Mohd Hussein. Senior Lecturer. Faculty of Law, Universiti Kebangsaan Malaysia. Email: finaz@ukm.edu.my ORCID: <https://orcid.org/0000-0002-1780-9426>

³ Ramalinggam Rajamanickam. Senior Lecturer. Faculty of Law, Universiti Kebangsaan Malaysia. Email: rama@ukm.edu.my ORCID: <https://orcid.org/0000-0003-4017-8826>

**Corresponding Author: bareq_montder@yahoo.com

A. INTRODUCTION

The digital age is characterized by the ubiquitous use of digital technology including smartphones, social media, e-commerce, and internet-connected devices (Lubis & Kartiwi, 2013). Daily activities, communications, financial transactions, and personal information are often concluded or stored online. The interconnected nature of the digital landscape increases the risk of data breaches (Bakhrudin et al., 2023; Petit, 2020) and cyber-attacks (Bradley, 2023; Younies & el Al-Tawil, 2020). Large-scale breaches compromise sensitive personal information, leading to identity theft, financial fraud, and other forms of cybercrime. Companies and online platforms often collect user data for personalized services and targeted advertising. While customization enhances user experience, concerns arise regarding the collection and utilization of personal information without explicit consent (Hamsin et al., 2023). Social media platforms encourage the sharing of personal details, thoughts, and experiences. Oversharing may lead to unintended consequences, such as invasion of privacy (Aissani, 2022; Saputra et al., 2022), stalking (Annadurai et al., 2022) or misuse of shared information (Osman, 2023). High-profile data breaches affecting major corporations and organizations have exposed sensitive personal information, such as names, addresses, and financial details. Sophisticated cyberattacks and hacking incidents contribute to concerns about the security of personal data (Onifade et al., 2019; Tiirmaa-Klaar et al., 2016). Such that stolen personal information can be exploited for identity theft (Light, 2021; Singh & Alshammari, 2020) and financial fraud (Masur & Trepte, 2021), leading to significant economic losses and reputational damage for individuals. Criminals may use compromised data to open fraudulent accounts, make unauthorized transactions, or engage in other forms of financial exploitations.

Similarly, governments may engage in large surveillance, raising concerns about citizen's privacy rights (Petit, 2020). The balance between national security and individual privacy becomes a crucial societal discussion. IoT devices, from smart home appliances to wearables, collect vast amounts of data (Annadurai et al., 2022; Romansky, 2022; Whaiduzzaman et al., 2022). The interconnectedness of these devices raises concerns about the security of personal information. The rise of IoT devices has expanded the scope of data collection, creating more entry points for potential privacy breaches (Kim et al., 2022; Whaiduzzaman et al., 2022). Online activities often leave digital footprints, eroding the anonymity traditionally associated with certain actions. Companies may monetize data by selling it to third parties for advertising or other purposes. Individuals may feel at loss of control over their personal information and online identities (Zhang et al., 2022). Hence, increased awareness of privacy issues led

to the development of data protection laws and regulations globally, such as the European General Data Protection Regulation (GDPR) (Jang & Newman, 2022; Romansky, 2022; Weber et al., 2020) and the California Consumer Protection Regulation Act (CCPA) (Cranor, 2021; Kaufman, 2022; Skowronski, 2022). Compliance with these regulations is essential for businesses and organizations to ensure responsible handling of personal data.

Concerns about online privacy can have psychological effects, including stress, anxiety, and a sense of vulnerability. Advanced data analytics and machine learning technologies enable extensive profiling and data mining (Jankovic & Curovic, 2023; Romansky, 2022). The potential for evasive data practices raises ethical concerns and the need for responsible use of emerging technologies. Individuals may alter their online behavior or self-censor due to privacy concerns. Privacy is recognized as a fundamental human right and is closely tied to ethical considerations (See Article 12 UDHR; Article 17 ICCPR; Article 8 ECHR). Respecting privacy aligns with principles of autonomy, dignity, and individuals' freedom (Teo, 2023). Therefore companies and organizations are increasingly expected to be transparent about their data practices and to prioritize user privacy. Privacy-conscious consumer may choose products and services based on companies' commitments to data protection (Radi, 2022).

Cultural norms and regional perspectives influence perceptions of privacy. In Islam, privacy is a spiritual injunction given to Muslims in the Al-Quran. Due to the importance of privacy to Muslim, the Quran provides thus on privacy:

“27. O you who believe, do not enter houses other than your own until you are sure to welcome and greet their occupants. That's what's best for you; maybe you will be reminded. 28. And if you find no one in it, do not enter it until you are given permission... 29. There is nothing wrong with you entering uninhabited houses in which there is comfort for you...” (Surat an-Nur: 27-29)

Privacy from the above verse is a mandate. Individuals should respect people's privacy and not to intrude whatsoever without consent (Saputra et al., 2022). Privacy is one of the Islamic principles and it falls within the concept of *aurah* which means space and privacy (Bakhrudin et al., 2023). Studies have been carried out on the Islamic perspective of privacy and personal protection. For instance Denny Suwondo (2023) in examining the Islamic perspective of the legal protection of personal data, argued that the essence of the Islamic perspective on protection of personal data is to maintain the use of information technology for the benefit of individuals and society. Privacy and trust within Islamic principle

as opined by Lubis and Kartiwi (2013), is as properly captured in the hadith narrated by Shahih Bukhari, book 62 no. 27 which clearly prohibits peeping into another person's house without permission. While Alizadeh (2018) is of the opinion that privacy is central to the nature and life of Muslims for the protection of culture and ideology as provided in the Quran. Muhammad and friends (2023) argued that the use of Sharia e-wallet in Indonesia is in compliance with Islamic principles for the protection of personal data. Osman in analyzing the right to be forgotten in Islam, concluded that despite the inadequacy of Qur'anic verses and divergent views of other scholars, the right to be forgotten can be defended under the Islamic principle of *satr or sitr*, the need to respect privacy (Osman, 2023). Therefore Islam prohibits the violation of both physical and personal life's privacy added Bagheri and Althabhwawi (2022). Shehu and friends (2018) are of the opinion that the use of social media has both *halal* and *haram* perspective of it, as such its usage should be regulated within Islamic principles. Similarly, Sherwani (2018) examined the right to privacy in Islam in relation to cyber security and Onifade, Akinwande and Shehu (2019) examined privacy in Islam in relation to hacking as a breach of privacy. However, research is lacking on the need for individuals particularly Muslims to imbibe the Islamic principle of *Amanah* (trust or honesty) in relation to individual's privacy and desist from *Ghibah* (gossip and backbiting).

B. METHODS

Using a doctrinal approach of legal research through analyzing existing literatures and other legal text, this article analyzed the Islamic perspective of online privacy and personal data protection with emphasis on *Amanah*, along conventional international data protection. It seeks to add to the discourse on the Islamic perspective of online privacy and personal data protection. Understanding and respecting diverse perspectives on privacy is crucial in a globally connected digital environment. Though global data flows and transnational data processing present challenges in ensuring consistent and robust data protection standards. Yet, harmonizing international approaches to privacy with the Islamic perspective of privacy becomes crucial in a globally interconnected digital environment.

C. RESULTS AND DISCUSSION

1. Islamic Principles Relevant To Online Privacy

Privacy enables individuals to exercise control over their personal information, protect their dignity, autonomy, and freedom of expression

(Škrinjarić et al., 2019). Privacy is a fundamental aspect of Islamic teachings (Lubis & Kartiwi, 2013; Osman, 2023; Saputra et al., 2022), and the Quran and Hadith contain several verses and sayings of Prophet Mohammad (PUH) that emphasize the importance of respecting individual privacy. Some relevant verses of the Quran and Hadith on privacy include:

a. Quran:

“O you who have believed, avoid much [negative] assumption. Indeed, some assumption is a sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of Repentance and Merciful.” (Surah Al-Hujurat 49:12). This verse highlights the prohibition of spying and backbiting (*Ghibar*), promoting a culture of trust and privacy. While respecting an individual’s privacy without any form of intrusion. “And they swear by Allah their strongest oaths that if they came to them a sign, they would surely believe in it. Say, ‘The signs are only with Allah.’ And what will make you perceive that even a sign came, they would not believe” (Surah Al-An’am 6:109). This verse emphasizes that certain matters are between individuals and Allah alone, highlighting the sanctity of personal beliefs and convictions. “O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. This is best for you, perhaps you will be reminded” (Ayah an-Nur (The Light) 24:27)

This verse encourages seeking permission before entering someone’s private space, promoting the concept of privacy in homes. This verse can be extended to seeking express consent before intruding one’s privacy including the collection, processing, storing and usage of one’s personal information (Denny, 2023; Osman, 2023; Saputra et al., 2022) which constitutes his/her privacy.

b. Hadith:

The Prophet Muhammad (PUH) said: “Beware of suspicion, for suspicion is the worst of false tales; and do not look for the others’ fault and do not spy, and do not be jealous of one another, and do not desert (cut your relationship with) one another, and do not hate one another; and O Allah’s worshipers! Be brothers (as Allah has ordered you!)” (Sahih al-Bukhari, 6066, Hadith 94).

The hadith highlights the Prophet guidance to avoid suspicion, finding faults in others, spying on someone’s privacy and Najsh and jealousy. As such private conversations that may exclude others should be avoided, promoting inclusivity and respecting the feelings of individuals.

The Prophet Muhammad (PUH) said: “If you guarantee me six things on your part, I shall guarantee you Paradise: Speak the truth when you talk, keep a promise when you make it, when you are trusted with something fulfill your trust, avoid sexual immorality, lower your gaze (in modesty), and restrain your hands from justice” (Sunan Abi Dawood). The Hadith emphasizes the importance of truthfulness and trustworthiness, including the fulfilment of entrusted information or secrets.

These verses and Hadith emphasize principles such as avoiding suspicion, refraining from spying prying into other’s affairs, seeking permission before entering private spaces, and maintaining trust and confidentiality. Islamic teachings promote a culture of respect for individuals’ privacy and trust in interpersonal relationships.

2. Islamic Principles Relevant To Privacy

The Islamic principles relevant to online privacy include *Sitr* (Respect for privacy), *Amanah* (Trustworthiness), *Ghibah* (Avoidance of backbiting), *Haram* (Avoidance of unlawful transactions).

a. *Sitr* or *Satr*

The Islamic concept of *Sitr*, which emphasizes respect for privacy, has implications in the digital context. As technology continues to play a significant role in modern life, it becomes crucial to apply *Sitr* principles to online interactions and digital spaces. Organizations and Individuals that collect and process data, should respect the digital boundaries of others, refraining from invasive actions such as unauthorized access to personal accounts, or cyberstalking. Respecting these privacy settings aligns with the concept of *Sitr* by giving individuals control over their digital presence similar to allowing data subject enjoy all their rights contained in Chapter 3 (Articles 12 to 23) of the GDPR. These includes transparency and modalities; information and access to personal data; rectification and erasure; right to object and automated individual decision-making; and restrictions. These rights all contribute to the right of control that a data subject can exercise under the GDPR. People should refrain from engaging in online gossip, backbiting, or spreading rumors about others, as it is in line with the Islamic principles of avoiding harm and maintaining the dignity of individuals. Participating in online discussions that disrespect or harm someone’s reputation, accessing and sharing unauthorized data, all goes against the spirit of *Sitr*.

Organizations should take measures to protect data subjects information collected and processed and individuals should also safeguard their personal data online, by using strong and unique passwords, enabling two-factor authentication (Al-Masalha et al., 2020; Koziol-McLain et al., 2018), and being cautious about sharing sensitive information. Similarly, respecting the personal data of others and refraining from attempting to access or exploit it aligns with the principles of trustworthiness (*Amanah*) and *Sitr*. Online conversations especially those of a private nature, should be treated with confidentiality. Just as private conversations in physical spaces are guarded, the same respect should be extended to digital communications. Promoting awareness about the importance of online privacy and the principles of *Sitr* can contribute to a culture of respect in the digital realm. Others should be encouraged to adopt responsible and ethical online behaviors aligns with Islamic teachings on communal well-being and mutual respect (Osman, 2023; Saputra et al., 2022). Avoiding the use of invasive technologies such as spyware, malware, or other tools that compromise the privacy of individuals is consistent with the principles of avoiding harm and respecting personal space.

Therefore, there is a need to strike a balance in the use of technology to ensure that it does not intrude on personal lives excessively is in line with the Islamic principle of moderation. Surveillance on digital communications at the expense of face-to-face interactions may impact the quality of relationships. Individuals should take action to report and address online harassment, bullying, or any form of harmful behavior. Upholding justice (*Adl*) (Denny, 2023; Sherwani, 2018) in the digital space aligns with Islamic principles and contributes to a safer online environment.

b. Amanah (Trust, honesty or sincerity)

Trust or *Amanah* in Arabic, is indeed considered a fundamental Islamic value and lays an important role in various aspects of individual and community life. The concept of trust is deeply rooted in Islamic teachings and is emphasized in both the Quran and the Hadith. Islam places a significant emphasis on trustworthiness as a noble character trait. Trustworthiness is linked to the concept of integrity, honesty, and fulfilling commitments.

The Quran in Surah Al-Anfal (8:27) says: “O you who have believed, do not betray Allah and the Messenger or betray your trusts while you know [the consequence]” The verse underscores the importance of not betraying of or not betraying trust, whether they are commitments to God, the Prophet, or to fellow human beings. Also Surah Al-Ma'idah (5:1): “O you who have believed, fulfill [all] contracts. Lawful for you are the animals of grazing livestock except for that

which is recited to you [in this Quran]...” This verse emphasizes the fulfillment of contracts and commitments, promoting trust in economic and social transactions.

In the Hadith, the Prophet Muhammad (PUH) is reported to have said: “The signs of a hypocrite are three: whenever he speaks, he tells a lie; and whenever he promises, he breaks his promise; and whenever he is entrusted, he betrays (roves to be dishonest).” This Hadith highlights the grave nature of betrayal of trust and identifies it as a sign of hypocrisy.

Trust is fundamental in economic transactions, and Islam encourages fair and transparent dealings (Lubis & Kartiwi, 2013). Honest trade, accurate measurement, and fulfilling contractual obligations are all aspects of trust in business. Trust is crucial in interpersonal relationships within families and communities (Badi, 2016; Desi Erawati, 2019). Including friendships and marriages. Being reliable, keeping confidences, and fulfilling promises are considered integral to trust in these relationships. Believers place trust in Allah, relying on Him for guidance, support and protection. This trust in the Divine is a fundamental aspect of Islamic spirituality. Betrayal of trust, whether in personal relationships or in a broader societal contexts, is strongly condemned in Islamic teachings. Betrayal is considered a breach of ethical conduct (Badi, 2016; Saputra et al., 2022). Hence, building trust within community is essential for its well-being. Cooperation, honesty, and mutual respect contribute to a cohesive and harmonious society. Fulfilling pledges and commitments is seen as an obligation in Islam. Breaking promises or betraying trust is considered a violation of Islamic ethics which should be avoided.

Imam Ahmad also narrated a hadith with a sound chain of narrators through Ubadah Ibnul-Samet that the Prophet (PBUH) said, “If you guarantee me six things on your part, I shall guarantee you Paradise: Speak the truth when you talk, keep a promise when you make it, when you are trusted with something fulfil your trust, avoid sexual immorality, lower your gaze (in modesty) and restrain your hands from injustice (Al-Ifta, n.d.; Badi, 2016).

This verse emphasizes truthfulness, honesty, keeping a promise and being trustworthy as tenets of Paradise. Individuals are admonished by this hadith to be trustworthy meaning to exercise *Amanah* in all their dealings. This is because not being trustworthy is equated with hypocrisy and the hypocrites will be punished but those with *Amanah* would be rewarded (See also Quran 33:24). As clearly stated in this Hadith:

“That Allah may reward the truthful for their truth and punish the hypocrites if He wills or accept their repentance” (Al-Ahzab: 24). Similarly, At-Tirmidhi, narrated a hadith with a sound chain of narrators that the Prophet (PBUH) said, “Truthfulness is tranquillity and falsehood is suspicion” (Al-Ifta, n.d.; Badi, 2016).

In the above hadith, truthfulness is illustrated with tranquillity (calmness, serenity, peace) while falsehood is akin to suspicion which must be avoided by individuals. Hence, when people deal with personal data of individuals, they must act with *Amanah* for their own peace, calmness and serenity while avoiding any form of suspicion by the data subject in the handling of their personal data that has been collected. This Islamic principle can be argued to be similar to the GDPR’s lawful, fair and transparent principle in the processing of personal data. Which should be restricted to the purpose of collection under Article 5(b) and 89 of the GDPR. While in the case of the CCPA, Section 1798.120 states that the data subject must be given the right to opt-out of sale of his data at any time without restriction. This means that if the individual adheres to *Amanah*, he will not breach or infringe on the right of a data subject’s right. Similarly, the data subject would be able to exercise his/her right to opt-out of sale without restriction. The purpose of data collection and processing would be for a fair and lawful purpose.

Ibn-Abul-Donya narrated on the authority of Mansour Ibnul-Mo’tamer that the Prophet (PBUH) said, “Seek truthfulness even if it will bring you to ruin; in it is your real salvation” (Al-Ifta, n.d.). From the above hadith, people should exercise *Amanah* at all times in his/her dealing with individual’s data collected, even if the honest and truthful usage of it would amount to loss on the part of his/her organization or business. For the reason that, doing so means their salvation. Individuals should ensure that when people give their trust (Badi, 2016; Mohamed & Zeki, 2023; Munawar et al., 2010; Onifade et al., 2019), it should be kept and managed honestly which is *Amanah*. Therefore it is better to stay with salvation than to lose salvation because of dishonesty or lack of truthfulness in processing of personal data that has been lawfully collected and stored. It is better for people to stay true, be truthful and leave with trustworthy people to save himself/herself. O you who have believed, fear Allah and be with those who are true,” (At-Tawbah: 119).

Those who are truthful and trustworthy are indeed righteous and the righteous have been promised a seat of honour to sit near the Sovereign in Paradise. He also said, “Indeed, the righteous will be among gardens and rivers, In a seat of honor near a Sovereign, Perfect in Ability,” (Al-Qamar: 54-55). Also, “It is enough for you that truthfulness will save you from evil, because ‘in

truthfulness lies safety.” Therefore, people who are part of and owners of organizations and business that are involved in the collection, storing and usage of personal data should be truthful and honest in their dealing. Those personal data collected should be used only for the purpose for which it was collected and nothing more. If they use it for another purpose without the consent to do so, they have breached their obligation of *Amanah* which is one of the six principles to paradise for the faithfuls (Bakhrudin et al., 2023; Mohamed & Zeki, 2023; Munawar et al., 2010; Onifade et al., 2019). That act would not only harm them in this world (resulting in a civil suit and heavy damages) but also the life after when they would lose paradise.

Additionally, in Islam, handling personal data is viewed as a form of trust, and individuals and organizations are expected to fulfill their responsibilities with utmost integrity and transparency (Badi, 2016; Jawi et al., 2016; Munawar et al., 2010). The principles of trust and responsibility in handling personal data aligns with the broader concept of *Amanah*. Individuals and organizations are obliged to safeguard the privacy of personal data entrusted to them. Respecting the confidentiality of personal information reflects the Islamic value of *Sitr*. Obtaining informed consent from individuals before collecting, or sharing their personal data is a fundamental principle similar to the need for consent before collecting and processing of data subject’s personal data under Article 7 & Recital 32 of the GDPR and S. 1798: 100 of the CCPR.

Transparency about the processes and uses of personal data aligns with Islamic ethical standards. Hence, it is important for organizations and businesses to ensure the accuracy of personal data and provide truthful information, because misrepresentation or manipulation of personal data goes against the principle of honesty and integrity in Islam. Also, as believers, personal data should only be collected and used for legitimate and specified purpose. Ensuring that data is not misused or repurposed without consent in line with responsible handling of data.

Similarly, there is need to establish clear policies for retention and disposal of personal data is essential. Unnecessary retention of data beyond its purpose may be considered a breach of trust. While ensuring that personal data that is collected is not used for unlawful activities or transaction is a responsibility. This is because engaging in illegal activities violates Islamic principles is strictly prohibited. Organizations and businesses especially believers should take responsibility for any mishandling or misuse of personal data is a fundamental Islamic principle. In the event of a data breach, promptly informing affected

individuals and taking corrective actions is a duty. Transparency about data breaches aligns with the principles of trust and responsibility within Islam.

c. *Ghibah (Backbiting and gossip)*

Ghibah is defined as speaking about someone in a way that they would dislike whether the information is true or false. It includes revealing someone's faults, shortcomings, or private matters in their absence. In Islam, *Ghibah* and gossip are strongly prohibited, and engaging in such behavior is considered sinful (Badi, 2016; Onifade et al., 2019; Osman, 2023; Sherwani, 2018). Islamic teachings emphasize the importance of guarding one's tongue and refraining from speaking ill of others. The prohibition of backbiting is rooted in various Quranic verses and Hadiths. For instance, Surah Al-Hujurat (49:12) as cited earlier prohibits assumptions, spying, or backbiting and draws a powerful analogy to eating the flesh of a dead brother, which highlights the repugnance of such actions.

In the Hadith, the Prophet (PUH) is reported to have said: "Do you know what backbiting is?" They said, "Allah and His Messenger know best". He then said, "It is to say something about your brother that he would dislike." Someone asked him, "But what is what I say is true?" The Messenger of Allah said, "If what you say about him is true, you are backbiting him, but if it is not true then you should have slandered him." This Hadith underscores that even if what is said is true, speaking about someone behind their back in a negative manner is considered backbiting.

Islam prohibits spreading rumors or unverified information about others. Spreading false information can lead to harming someone's reputation and is contrary to the principles of justice. Islam also emphasizes the preservation of individual dignity and honor. Backbiting and gossip undermines this dignity, causing harm to individual's reputation. Therefore, believers are encouraged in Islam to seek forgiveness for engaging in backbiting, especially repentance and forgiveness from the person being backbitten upon as a necessary step to rectify the harm caused. This is because, backbiting and gossiping may lead to negative consequences in the Hereafter. Islam warns about the potential punishment for such actions in the afterlife. *Ghibah* can also lead to discord and animosity among individuals and within community (Badi, 2016; Onifade et al., 2019). Islam promotes brotherhood, unity and positive interpersonal relationships. Reflecting on one's own imperfections and shortcomings should discourage engaging in backbiting. None is free from faults, and humility is key to respect of Islamic teachings.

In relation to online privacy and personal data protection, Muslims are urged to adhere to Islamic ethical principles even in virtual spaces (Badi, 2016; Bakhrudin et al., 2023; Desi Erawati, 2019). Individuals are encouraged to be mindful of their speech in online discussions and social media platforms. Refraining from backbiting, spreading rumors, or engaging in negative discussions about others is vital. Islam emphasizes *Sitr*, which extends to online spaces. Individuals are obliged to avoid the sharing of personal information or discussing others' private matters without their consent in accordance with Islamic principles. Before sharing information or news online, Muslims are encouraged to verify its authenticity. Spreading unverified information can lead to harm and may fall under the prohibition of spreading rumors.

Since online discussions often involve diverse perspectives, people are reminded to avoid negative assumptions about others' intentions (Isah Shehu et al., 2018; Lubis & Kartiwi, 2013). Upholding a positive and respectful tone in digital conversations in line with Islamic ethics. As such, individuals should contribute positively to online discussions, promoting knowledge sharing, understanding, and constructive dialogue. Avoid engaging in conversations that may lead to *Ghibah* or negative speech. When engaging in online activities that involves sharing personal information, seeking permission from individuals is considered respectful. This is because, consent is important and must be sought before spreading one's personal information. Social media platforms and other forums often provide privacy settings. Individuals should respect these settings and avoid accessing or sharing information that is not meant for public view. Similarly, Islam encourages the promotion of positive interactions and discourages engaging in discussions that may lead to harm or discord as earlier highlighted. Hence, positive behavior in online spaces contributes to a harmonious digital environment. People should therefore uphold trustworthiness and honesty in business transactions. While avoiding deceptive practices and providing accurate information.

d. Haram (engaging in Unlawful activity)

Sharia provides a robust framework derived from the Quran and Sunnah. It encompasses ethical guidelines and legal principles that govern various aspects of personal and communal life (Badi, 2016; Munawar et al., 2010). Individuals are instructed to adhere to ethical and legal standards. With greater emphasis on the importance of justice, honesty, and ethical behavior. Islam categorically prohibits engaging in actions regarded as *Haram*, based on clear guidance from the Quran and Hadiths. Some examples of *Haram* activities includes consuming alcohol,

engaging in usury (*Riba*), committing theft, and participating in fraudulent practices. Islam emphasizes justice and fair dealing in all transactions and interactions. Unlawful activities often involving injustice (Hamsin et al., 2023; Saputra et al., 2022), exploitation, or harm to oneself or others, which contradicts Islamic principles. Muslims are instructed to respect and abide by the laws of the land in which they reside.

Following local laws and legal systems is considered part of a Muslim's responsibility and obedience to authority. Furthermore, engaging in fraudulent activities or deception is strictly prohibited and people are expected to conduct their businesses and personal affairs with honesty and integrity (Bakhrudin et al., 2023; Hamsin et al., 2023). Actions that harm oneself or others are inconsistent with Islamic principles of preserving life. More so that, individuals are accountable for their personal conduct, and engaging in unlawful activities is considered a breach of moral and ethical standards. Engaging in unlawful activities have spiritual implications, as such individuals should seek forgiveness and strive for righteous conduct to safeguard themselves from the consequences in the Hereafter.

Therefore, avoiding unlawful transactions aligns with the prohibition of engaging in Haram (Isah Shehu et al., 2018). Muslims should gain knowledge of Islamic financial principles, such as the prohibition of *Riba*, *Gharar* (excessive uncertainty), and involving in Haram substances. Before engaging in any online financial transactions, individuals should verify the legitimacy of the platform or website. They should be sure that the platform complies with legal and ethical standards of data protection regulation and Islamic principles, especially in financial matters. Be cautious about financial transactions that involve interest, because *Riba* is strictly prohibited in Islam (Bakhrudin et al., 2023). Verify the terms and conditions of loans, investments, or financial products to ensure adherence to Sharia principles. When engaging in online commerce, verify the business practices of e-commerce platforms. Ensure that the products or services offered do not involve unlawful activities or violate Islamic principles.

People should be mindful of the content and advertisements on digital platforms. Avoid engaging in transactions that promote or involve Haram activities, such as sale of prohibited substances and services. Exercise caution when sharing personal information online. Avoid transactions or engagements that require the sharing of sensitive data without proper security measures. Before participating in online investments, thoroughly evaluate the legitimacy and compliance of the investment opportunities with Islamic financial principles. Be wary of schemes that promise unrealistic returns or involve speculative risk

activities. Carefully read and understand terms and conditions of any online transactions. Ensure that the terms align with ethical and legal standards and do not violate any prohibited activities. While refraining from engaging in online activities that involve gambling or speculative transactions. This is because gambling and *Gharar* are prohibited in Islam (Bakhrudin et al., 2023; Hamsin et al., 2023). Hence, individuals are expected to be vigilant, seek knowledge, and make informed choices that are in line with religious and ethical values in the digital realm.

3. Legal Compliance and Regulatory Framework

a. Comparative Analysis

Islamic principles and existing data protection laws share common goals in safeguarding individual privacy, promoting ethical conduct, and ensuring the responsible handling of personal information. While the foundations may differ, there are areas of alignment between Islamic principles and the principles embedded in modern data protection laws. Similarities can be found in the following areas:

i. Respect for privacy (Sitr) and Data Minimization

Islamic principles emphasize the importance of respecting privacy and avoiding unnecessary disclosure of personal matters (Sherwani, 2018). Data protection regulation laws on the other hand advocates for data minimization (Filipec et al., 2022; Pendaroska, 2021). Organizations are required to collect and process only the data that is necessary for the specific purpose for which the data was collected.

ii. Informed consent (permission) and consent in data protection

Under Islamic law, consent is emphasized before engaging in certain actions, this shows the importance of respect for individual's autonomy. Including entering into individual homes. Data protection regulations also require obtaining informed consent from individuals before collecting, processing, or sharing individual's personal data.

iii. Avoidance of backbiting (Ghibah) and Data confidentiality

In Islam, backbiting and gossiping is prohibited. Muslims are not expected to engage in backbiting or disclosing individual's personal information without obtaining permission. While data protection regulations require individuals, organizations and business to adhere to the principle of

confidentiality (Bagheri & Althabhwawi, 2022; Mohamed & Zeki, 2023). They should not disclose, sell or use data subject's personal information without express consent or beyond the purpose for which the data was collected.

iv. *Avoidance of Unlawful Transaction (Haram) and Legitimate processing*

Unlawful transactions are considered haram in Islam and Muslims are prohibited from doing acts that are considered haram. Data protection regulations expect that for data to be collected and processed, it must have been legally collected and must be processed legitimately as part of the principle of legal, fair and transparent principle of data processing under Article 89 of the GDPR.

b. Qiyas (analogical reasoning)

Qiyas involves deriving legal rulings for new issues through analogies with established cases from the Quran and Sunnah. Qiyas, often referred to as analogical reasoning, is a method of legal reasoning in Islamic Jurisprudence (*fiqh*) where the ruling of a known issue is applied to a new or similar issue (Badi, 2016; Munawar et al., 2010). It involves making an analogy between a known situation (the original case) and a new situation (the analogous case) to derive a legal ruling. Qiyas is one of the four primary sources of Islamic law, alongside the Quran, Sunnah, and Ijma. It is one of the pillars of Islam alongside the Quran, Sunnah, and Ijma. This method relies on the identification of the underlying reason behind a ruling and applying it to a similar situation (Falak et al., 2024). Qiyas ensures the adaptability and relevance of Islamic law in changing circumstances. As such, for discussions of this nature that involve applying Islamic law principles to technology-oriented issues, Qiyas is relied upon.

The Qur'an and the Sunnah (Hadith) are the principal sources of Islamic law and are considered the Muslim way of life. Every discussion aimed at solving a particular problem should identify the source (*dalil*) from both before reaching a decision, with the Qur'an and Sunnah ranking highest among the primary sources, *ijma*, or consensus among Muslim jurists, and *qiyas*, or modification, ranking lower (Lubis & Kartiwi, 2013). In some cases, when it becomes difficult to reach a consensus on a single issue due to a variety of factors, including the Qur'an and Sunnah as sources that appear to contradict one another, the variations in methods or understandings of thought (*madh'hab* vs. *minhaj*), and social customs (*urf*). It becomes imperative to reflect on the prophet's (PBUH) understanding of tradition. Because of this, it's critical to reflect on the prophet's (peace be upon him) historical understanding of the original source and their actual practice. In this way, based on the foundational principles and teachings

of Islam, the scholars (ulama) formulate recommendations and lay down guidelines (fatwas) (Hamsin et al., 2023; Lubis & Kartiwi, 2013). The issue of online privacy and personal data protection falls within the issues that guidelines and recommendations can be formulated on by the *ulama's*.

The evidence presented by scholars will be confirmed and double-checked by the Muslim community against rationally supported or cross-referenced evidence. In situations such as where the problems are related to advancements in technology, and some cases that have not been adequately and clearly explained in the main sources (Lubis & Kartiwi, 2013), qiyas is utilized to find solution. Hence, since technology supports and aids people for their own advantage, centred on Islamic principles, its use in day-to-day activities has been encouraged. One could argue that technology including the internet, social media and other emerging technologies like big data analytics, Artificial intelligence and Internet of Things are gifts from Allah to humanity, and it is the responsibility of humankind as khalifah (leaders) to give thanks to Allah for this gift. Therefore, the right to privacy from Islamic perspective within analogical deductions or reasoning can be subdivided into the following categories: maintaining one's dignity and privacy (*stir*) individuals should neither reveal information about others nor about themselves as a mark of safeguarding privacy (Falak et al., 2024), maintaining one's integrity and trust (*Amanah*) when individuals and organizations specify the purpose of collection and processing of personal data, integrity entails that they should not derogate from the purpose, avoiding gossip and backbiting (*Ghibah*), and abstaining from illegal activity (*haram*).

i. Key elements of Qiyas

Key elements of Qiyas includes *Asi* (Original case); *Hukm* (Legal ruling); *Illah* (Effective cause); and *Mujtahid* (Scholar qualified for *Ijtihad*). Analogical reasoning in Qiyas is based on a recognised legal judgement from the Quran, Sunnah, or *Ijma*. The “*hukm*” (ruling) is the legal decision that resulted from the initial case. It could be deemed necessary (*wajib*), forbidden (*haram*), acceptable (*halal*), or advised (*mustahabb*). The logic or basis for the initial case's court decision is known as the effective cause. Applying the parallel to the current scenario requires determining the effective cause (*Illah*). For Qiyas to be implemented, an expert jurist, or *mujtahid*, must be able to execute *ijtihad* (independent legal reasoning) and use analogical reasoning.

ii. Criticism and Limitations of Qiyas

Qiyas, has faced criticism and limitations of application. One of which is the fact that identifying effective cause can be subjective, and scholars may differ in their interpretation, leading to different outcomes. Qiyas is applicable to issues not explicitly covered in the Quran or Sunnah. However, its scope is limited to cases where an effective cause can be identified. Critics argue that Qiyas may not be flexible enough to address new and evolving situations, especially in the context of rapidly changing societal norms and technological advancements. Differential legal schools within Islam may apply Qiyas differently, leading to variations in legal rulings (Lubis & Kartiwi, 2013).

Critics argue that the reliance on fixed, historical interpretations of sources like Quran and Sunnah can hinder flexibility and adaptation to contemporary legal issues. It limits the reliance on Islamic law in a rapidly changing world. Also, the divergent views of the different schools of thought often complicate the development of a unified approach, which leads to confusion over the appropriate interpretation to be employed in a modern legal context. These criticisms are both internal and external. In internal criticism, the main issue is on the interpretive methodologies. It deals with debates between traditionalists advocating strict adherence to classical texts and reformists promoting contextual reinterpretations. While the external criticisms deal with non-Muslim perspectives. It focuses on issues of legal pluralism. Challenging the compatibility of Islamic legal principles with secular legal systems in multicultural societies. However, Islamic scholars have responded to these criticisms by reinterpreting text, engaging in dialogue, and advocating for reform. These scholars have provided nuanced interpretations that reconcile Islamic legal principles with contemporary context and values. This has been achieved through Islamic banking and evidence in the takaful system too

Despite criticisms, Qiyas remains a valuable tool in Islamic legal reasoning, providing a mechanism for addressing contemporary issues in light of established principles from the Quran and Sunnah. Scholars exercise caution and diligence when employing Qiyas, recognizing its role in expanding legal reasoning beyond explicit textual sources.

c. Extending Legal Principles to Address Novel Technological Challenges

Extending legal principles to address novel technological challenges is a complex and ongoing process, requiring a careful balance between upholding established legal frameworks and adapting to emerging issues resented by technological advancements. In the context of Islamic law, the same principles

apply, with the additional consideration of aligning legal solutions with Islamic ethics and values. Under Islamic law, there are several key considerations for extending legal principles to address novel technological challenges. They include: Ijtihad (Independent reasoning); Maqasid al-Sharia (Objectives of Islamic Law); Qiyas (Analogical reasoning); Ijma (Consensus); Maslaha (Public interest); Digital Tawakkul (Reliance on Allah).

d. Applying Qiyas to Ensure Ethical Practices

Applying Qiyas within the framework of Islamic jurisprudence can be a valuable approach to ensure ethical data practices in the digital age. While Qiyas is traditionally applied to derive legal rulings, its principles can also be extended to address contemporary ethical challenges, including those related to the collection, processing, and use of personal data (Abdallah et al., 2021; Lubis & Kartiwi, 2013).

1). *Original case (Asl)*: For instance, the consumption of intoxicants is prohibited based on clear Quranic verses and hadiths (Abdallah et al., 2021; Khan et al., 2018).

- a) Context: The prohibition of harming oneself or others in Islam (*mafsadah*).
- b) Legal ruling (Hukm): It is prohibited (haram) to engage in actions that cause harm to oneself or others (Hamsin et al., 2023; Isah Shehu et al., 2018).
- c) Effective Cause (Illah): The effective cause is the prevention of harm and the promotion of well-being.

2). *Analogous Case (New Scenario)*:

- a) Context: The collection and use of personal data in digital environments.
- b) Application of Qiyas:
 - i. Identify similarities: Recognize similarities between the original case and the new scenario. In both cases, the emphasis is on preventing harm and promoting well-being.
 - ii. Establish effective cause: In the context of personal data, the effective cause is the privacy, security, and ethical use of individuals' personal information to prevent harm.
 - iii. Derived ethical guidelines: Based on the original ruling and effective cause, derive ethical guidelines for the collection, processing, and use of personal data (Munawar et al., 2010; Saputra et al., 2022). This may include principles of transparency, consent, data minimization, and protection against unauthorized access.

- iv. Consider potential harm: Assess potential harm to individuals or society that may arise from unethical data practices (Badi, 2016). This may include privacy violations, identity theft, or misuse of sensitive information.
- v. Promote well-being: Ensure that data practices contribute to the well-being of individuals and society. This involves safeguarding individuals' rights, respecting their autonomy, and fostering trust in digital interactions.
- vi. Involve ethical review: Implement mechanisms for ethical review of data practices involving scholars or ethical committees to assess compliance with Islamic values and principles (Saputra et al., 2022).

3). Case study Analysis

a). Application of Qiyas in Islamic Finance: an example is the Islamic and finance industry in Malaysia (Falak et al., 2024). The Core Principles: Qiyas uses analogical reasoning to derive legal rulings not explicitly addressed in the Quran and Hadith. For instance, Islamic finance institutions use Qiyas to determine the permissibility of modern financial products like Islamic bonds (Sukuk) based on principles derived from Sharia-complaint contracts outlined in classical texts (Falak et al., 2024).

b). Shariah e-wallet (Hamsin et al., 2023). Sharia digital payment in the field of Islamic economics. For instance, Indonesia has successfully employed a Sharia e-wallet, and the system complies with Islamic principles as stated in the Fatwa of the National Sharia Council (Hamsin et al., 2023). Indonesia has successfully achieved, compliance, security, and personal data protection via comprehensive government regulations through Bank Indonesia and the Financial Service Authority.

c). In Islamic finance for instance, the Core Principle for Islamic. Finance Regulations (CPIFR) sets out necessary conditions for effective banking supervision such as the fact that Islamic banks must include the frameworks for recovery and resolutions (IMF, 2018). The key principles governing Islamic banking include: (1) Principle of equity: prohibition of predetermined payments (*riba*) and prohibition of excessive uncertainty (*gharar*) manifested by contract ambiguity or elusiveness of pay-off (Muhammad & Elesin, 2022); (2) Principle of participation: investment return should be earned in tandem with participation in productive activity and based on the prohibition of *riba*; (3) Principle of ownership: It is hitched on "do not sell what you do not own." You cannot dispose of a property except based on rights. This practical application is similar to a data subject's right of "do not sell" link and compliance obligations of S.

1798:135 of the CCPA. Islamic finance is also known as asset-based financing, which shows a link between finance and the real economy (IADI, 2021). It also requires preservation and respect for property rights, as well as upholding contractual obligations by understanding the sanctity of contracts similar to the requirement of *Amanah*.

4). *Criticisms and Challenges to Qiyas application*

a). Subjectivity in identifying harm: Identifying harm can be subjective, and interpretations may vary. It requires careful consideration of potential consequences.

b). Technology complexity: Applying Qiyas to technology-related issues may be required due to the understanding of the digital landscape, posing challenges for scholars unfamiliar with intricate technological details (Denny, 2023; Sherwani, 2018).

c). Rapid technological evolution: The rapid evolution of technology may outpace traditional legal and ethical frameworks. Regular reviews and adaptability are essential.

d). Diverse perspectives: Different scholars or schools of thought may have varying perspectives on the application of Qiyas to specific technological issues.

Applying Qiyas to ethical data practices involves a thoughtful consideration of the principles derived from the prohibition of harm and the promotion of well-being in Islamic jurisprudence (Bakhrudin et al., 2023; Onifade et al., 2019). By incorporating these principles, ethical data practices can be aligned with Islamic values, ensuring the responsible and respectful handling of personal information in the digital realm.

4. Implementation Challenges and Solutions

Implementing privacy protection relying on the Sharia principle is not without challenges. These challenges include the rapid advancement of technology which has both negative and positive consequences. Compatibility to international human rights like privacy protection and adapting to rapidly changing social dynamics. As well as balancing technological advancements with conventional and Islamic ethical considerations. More so technology comes with novel issues that require constant review of legal frameworks to contain them. Therefore, Islamic leaders must play an important role in addressing these challenges as argued in this article.

Similarly, there are challenges to reliance on Qiyas in contemporary discourse. For the reason that the different Islamic schools of thought have their various views. The major schools of thought are: 1) the Hanafi School founded by Imam Anu Hanaf, known for its emphasis on reason and consensus (Ijma). It employs Qiyas (analogical reasoning) extensively to conclude on issues, it prioritizes public interest (maslaha) and flexibility in interpretation. 2) The Maliki was founded by Imam Mali Ibn Anas and the school is rooted in the legal tradition of Medina. It emphasizes local custom (urf) and public welfare (maslaha) in its legal reasoning. 3) The Shafi'I school was founded by Imam al-Shafi'I and emphasizes the Quran, Sunnah, Ijma, and Qiyas in its legal methodology. It seeks to harmonize textual evidence with rational reasoning and is therefore very rigid. 4) The Hambali School was founded by Ahmad Ibn Hambal and the school is known for its strict adherence to textual sources the Quran and Sunnan and rigorous application of Qiyas. It emphasizes literal interpretation and conservation in legal rulings and relies less on consensus (Ijma)

a. Rapid Advancement in Technology and its Impact on Privacy

Rapid technological advancements have significantly impacted privacy, introducing both benefits and challenges to individuals and society. These advancements have many domains, including information technology, communication, artificial intelligence, biotechnology, and the Internet of Things (IoT) (Kovalenko, 2022; Whaiduzzaman et al., 2022).

1). Positive impact. Advancements enable more efficient and convenient services such as online shopping, communication, and access to information. Progress in biotechnology has contributed to medical breakthroughs, personalized medicine, and improved healthcare outcomes. Technology facilitates innovative educational tools and platforms, enhancing learning opportunities and accessibility. Social media and instant messaging platforms connect people globally, fostering communication and collaboration (Isah Shehu et al., 2018; Onifade et al., 2019). Also, IoT and smart technologies contribute to the development of smart cities improving infrastructure, transportation, and public services.

2). Negative impact. Pervasive data collection and surveillance, often conducted by governments and corporations, raise concerns about the loss of personal privacy. The increasing connectivity and reliance on digital systems expose individuals to cybersecurity threats, leading to unauthorized access and data breaches. The use of biometric data, including facial recognition, raises privacy concerns as individuals may be identified and tracked without their

knowledge or consent. Automated decision-making systems and algorithms may perpetuate biases (Dai & Boroomand, 2022; Kaur et al., 2018), leading to unfair and discriminatory outcomes, especially in areas like employment, finance, and law enforcement. Likewise, social media platforms, while enhancing connectivity, can be sued to invade privacy through the authorized sharing of personal information, cyberbullying, and surveillance (Hakkala & Koskinen, 2022; Petit, 2020; Younies & el Al-Tawil, 2020). Technologies often erode the ability to remain anonymous online, impacting individual's ability to engage in private activities without scrutiny. The widespread use of smartphones and location-based services raises concerns about constant tracking and the potential misuse of this information. Profiling and behavioral analytics, often used in advertising and marketing, may infringe on individuals' privacy by creating detailed profiles based on their online activities.

3). Privacy protection measures. Governments and regulatory bodies across the globe have implemented data protection regulations like the GDPR and the CCPA, to safeguard individuals' rights regarding their data (Filipec et al., 2022; Kaul, 2019; Ortega, 2022). Integrating privacy considerations into the design of technologies, and ensuring that privacy features are embedded from the outset is paramount. Strong security measures should be implemented to protect sensitive data from unauthorized access and cyber threats. Similarly, transparency should be promoted and users be given control over their personal information through informed consent mechanisms. Ethical guidelines and standards should also be established for the responsible development and deployment of technologies, including AI and algorithmic. Public awareness should be increased while advocacy for privacy rights and organizational accountability should be upheld for unethical or invasive practices using legal and ethical means.

b. Balancing Technological Innovation with Islamic Ethical Considerations

Balancing technological advancement with Islamic principles is another implementation challenge. For the reason that it requires navigating the intersection of technological innovations with Islamic teaching, values and principles. This process ensures that innovations align with ethical guidelines derived from Quranic principles, Sunnah, and broader Islamic jurisprudence. Including fundamental values like justice, compassion, honesty, and respect for human dignity. Develop and deploy Artificial Intelligence and automation technologies in a manner consistent with Islamic ethics, avoiding harm, discrimination, and unjust decision-making (Denny, 2023; Lubis & Kartiwi, 2013; Onifade et al., 2019). Also, there should be the ethical handling of personal data,

respecting privacy rights and preventing unauthorized access. Align data practices with Islamic principles related to *Amanah*, and avoidance of harm.

Furthermore, innovations in areas like finance and fintech should adhere to Sharia-complaint principles, avoiding *Riba* and engaging in ethical financial transactions. Develop ethical guidelines for biotechnological advancements, emphasizing the preservation of life, respect for human dignity, and adherence to Islamic medical ethics (Grosu & Bubuic, 2017; Mohamed & Zeki, 2023). Promote ethical communication in the digital realm, respecting principles of honesty, and integrity, and avoiding harmful content. So that cyberbullying and misinformation would be avoided among people. Similarly, transparency, fairness, and accountability in AI-driven decision-making processes should be ensured and discrimination should be prevented. Caution should also be exercised in the deployment of surveillance technologies, ensuring they are being used responsibly and ethically, bearing in mind the need to uphold the right to privacy (*Sitr*). At the same time, innovations should consider environmental sustainability, reflecting the Islamic principles of *Khalifah* (stewardship) and the responsibility to preserve the earth. This way, a harmonious balance can be achieved, contributing to the well-being of individuals and society.

c. Role of Islamic leaders as a solution

Islamic leaders play a crucial role in creating awareness of online privacy by leveraging their influence, knowledge, and platform to educate and guide their communities. As trusted figures, they can highlight the ethical and Islamic considerations related to online activities, personal data protection, and responsible digital behavior by:

- 1). Incorporating privacy in Sermons and religious discourses, through connecting relevant Quranic verses, hadiths, and Islamic principles to the importance of respecting privacy in the digital age. Speak out against cyberbullying and online harassment, emphasizing the importance of treating others with respect. While highlighting the Islamic prohibition of harming others through speech and actions, even in the digital realm.

- 2). Issuing Fatwas and ethical guidelines. They should provide authoritative guidance through fatwas and ethical guidelines specifically addressing online privacy concerns by clarifying Islamic stance on respecting other's privacy, securing personal information, and the ethical use of technology. Instill the concept of digital *Tawakkul* (Reliance on Allah), emphasizing trust in Allah while taking responsible actions online. Connect the reliance on Allah with the ethical use of technology, and personal responsibility.

3). They should organize educational workshops and Seminars focused on online privacy and digital ethics. While covering topics such as secure online practices, the Sharia perspective on privacy, and the ethical use of the social media. Encourage content creators within the community to produce ethical and respectful digital content. Highlight the potential impact of content on privacy, reputation and Islamic values. Similarly, they can advocate for the inclusion of online privacy and digital ethics topics in Islamic education curricula. As well as work with educational institutions to integrate these themes into the broader Islamic studies curriculum.

4). Collaborate with technology experts to understand and communicate the potential risks and best practices related to online privacy. Host joint sessions where Islamic leaders and technology experts address the intersection of technology and ethical considerations.

5). Leverage social media platforms to disseminate information on online privacy. Share informative content, tips, and reminders about responsible online behavior, utilizing platforms with a wide reach.

Islamic leaders, through their guidance and influence, can contribute significantly to building a community that is mindful of online privacy and digital ethics. By incorporating these considerations into religious teachings and community initiatives, they play a vital role in shaping a responsible and ethically conscious digital society.

D. CONCLUSION

The exploration of online privacy and personal data protection from an Islamic perspective delves into the intersection of digital advancements and Islamic ethics. Guided by fundamental Islamic principles such as *Amanah*, *Sitr*, *Ghibah*, and *Haram*, the analysis extends across various aspects of online interactions. From *Ghibah* to *Haram*, the principles of Sharia law provide a comprehensive guideline for ethical conduct in the digital realm. Classical Islamic jurisprudence rooted in Quranic teachings and Sunnah, establishes the foundation for addressing contemporary challenges. The application of Qiyas ensures a dynamic response to technological changes, maintaining alignment with overarching Islamic values. The commitment to *Amanah* underscores the responsibility of individuals and entities in safeguarding personal information, emphasizing ethical considerations in data handling.

In conclusion, the synthesis of Islamic principles and digital ethics creates a robust guide for navigating the complexities of online privacy and personal

data protection. As technology evolves, the adaptability of Sharia law principles proves crucial in addressing novel challenges while upholding timeless values of justice and respect for human dignity. The engagement of Islamic leaders in raising awareness, the integration of ethical guidelines, and the promotion of responsible digital citizenship contribute to a harmonious coexistence of technological innovation and Islamic values. Therefore, to foster a holistic approach, ongoing collaboration between religious scholars, technological, and policymakers is imperative. By aligning legal frameworks, educational initiatives, and technological innovations with Islamic ethical considerations, societies can strive toward a digital landscape that reflects the principles of justice, accountability, and compassion outlined in Islamic teachings. This dynamic equilibrium ensures not only legal compliance but also the ethical flourishing of individuals and communities in the digital age.

The study hereby recommends future direction and policy implications to align privacy protection with Islamic principles summarized in Table 1 below.

Table 1. Future Direction and Policy Implication

FUTURE DIRECTION AND POLICY IMPLICATION			
S/N	Items	Implication	Practice
1.	Future Direction	Develop an Islamic-centric data privacy framework	establish guidelines and standards that integrate ethical principles into data privacy practices
		Islamic-based data protection certification	create a certification program for organizations that adhere to Islamic data privacy principles
		Research on Islamic perspectives on emerging technologies	explore Islamic ethical perspectives on AI, blockchain, and IoT to inform data privacy practices
		Capacity building and awareness	educate policymakers, organizations, and individuals on the importance of integrating Islamic ethical principles into data privacy practices
2.	Policy-Makers	Incorporating Islamic principles into national data protection laws	amend existing laws to reflect Islamic ethical principles such as the concept of "Amanah" (trustworthiness)
		Establish Islamic-centric data protection authorities	create regulatory bodies that oversee data privacy practices and ensure compliance with Islamic principles
		Developing Islamic-based data privacy guidelines for organizations	provide guidelines for organizations operating in Muslim-majority countries to ensure compliance with Islamic ethical principles as obtainable in Islamic banking practices
3.	Organizations	Conduct Islamic-centric data privacy impact assessments	assess data privacy practices to ensure compliance with Islamic ethical principles
		Developing Islamic-based data privacy policies	establish policies that reflect Islamic principles, such as transparency, accountability, and fairness
		Providing Islamic-centric data privacy training	educate employees on Islamic data privacy principles and practices
4.	Technology Developers	Design Islamic-centric data privacy features	incorporate Islamic ethical principles into technology design, such as data minimization and anonymization

		Develop Islamic-based data privacy tools	create tools that help organizations comply with Islamic data privacy principles, such as data protection software
		Conduct Islamic-centric data privacy research	explore Islamic perspectives on emerging technologies to inform data privacy practices

REFERENCES

Abdallah, A., Rahem, M. A., & Pasqualone, A. (2021). The multiplicity of halal standards: a case study of application to slaughterhouses. *Journal of Ethnic Foods*, 8(1). <https://doi.org/10.1186/s42779-021-00084-6>

Aissani, R. (2022). Anti-Cyber and Information Technology Crimes Laws and Legislation in the GCC Countries: A Comparative Analysis Study Of The. *Journal of Legal, Ethical and Regulatory Issues*, 25(1), 1–14.

Al-Ifta, E. D. (n.d.). *Truthfulness: The hard way to Paradise*. Retrieved March 12, 2024, from dar-alifta.org/en/article/details/258/truthfulness-the-hard-way-to-paradise

Al-Masalha, H., Hnaif, A., & Tarek, K. (2020). Cyber-crime effect on jordanian society. *International Journal of Advanced Soft Computing Applications*, 12(3), 2074–8523.

Alizadeh, H. (2018). The Concept of privacy and space in Kurdish cities. In T. Edensor & M. Jayne (Eds.), *URBAN THEORY A world of cities* (Issue February 2014, pp. 29–372). Routledge, Taylor and Francis Group New York.

Annadurai, C., Nelson, I., Devi, K. N., Manikandan, R., Jhanjhi, N. Z., Masud, M., & Sheikh, A. (2022). Biometric Authentication-Based Intrusion Detection Using Artificial Intelligence Internet of Things in Smart City. *Energies*, 15(19). <https://doi.org/10.3390/en15197430>

Badi, J. A. (2016). Commentary of forty Hadiths of An Nawawi. *Islamic Learning Foundation*, 220. <http://fortyhadith.iiu.edu.my/>

Bagheri, P., & Althabhwawi, N. M. (2022). Islamic and European Perspectives on Data Privacy in Online Contracts. *European Data Protection Law Review*, 8(3), 377–385. <https://doi.org/10.21552/edpl/2022/3/7>

Bakhrudin, B., Margolang, F. I., Sudarmanto, E., & Sugiono, S. (2023). Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications. *West Science Law and Human Rights*, 1(04), 166–172. <https://doi.org/10.58812/wslhr.v1i04.323>

Bradley, L. P. (2023). Was the Colonial Cyberattack the First Act of Cyberwar Against the U.S.? Finding the Threshold of War for Ransomware Attacks. *St. John's Law Review*, 96, 487–487. <https://www.nytimes.com/>

Cranor, L. F. (2021). Informing California privacy regulations with evidence from research. *Communications of the ACM*, 64(3), 29–32.

- <https://doi.org/10.1145/3447253>
- Dai, D., & Boroomand, S. (2022). A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. *Archives of Computational Methods in Engineering*, 29(2), 1291–1309. <https://doi.org/10.1007/s11831-021-09628-0>
- Daoud, H. S. (2021). Civil liability for social media hacking. *Imam Ja'afar Al-Sadiq University Journal of Legal Studies*, 1(1), 255–283. <https://www.iasj.net/iasj/issue/13269>
- Denny, S. (2023). The Legal protection of personal data in Islamic perspective. *International Journal of Law Reconstruction*, 7(2), 221–230.
- Desi Erawati, L. (2019). Social Media and Communication Ethic in Islamic Perspective. *Epistemé: Jurnal Pengembangan Ilmu Keislaman*, 14(1), 27–46. <https://doi.org/10.21274/epis.2019.14.1.27-46>
- Falak, H., Faizi, S., & Sfarish, H. (2024). *The Core Principles of Islamic Jurisprudence within Legal Theory : A Comprehensive Analysis*. 11(2), 57–72.
- Filipec, O., Alves, M. P., Heck, L. N., & Parma, G. D. (2022). Personal Data Protection in Brazil: How Much Europeanization? *International and Comparative Law Review*, 22(2), 81–104. <https://doi.org/10.2478/iclr-2022-0016>
- Grosu, R., & Bubuioc, V. (2017). The role of internet and social media in recruitment in certain Islamic terrorist organizations. Cases of Al Qaeda and ISIS. *Central and Eastern European EDem and EGov Days*, 325, 179–188.
- Hakkala, A., & Koskinen, J. (2022). Personal data protection in the age of mass surveillance. *Journal of Computer Security*, 30(2), 265–289. <https://doi.org/10.3233/JCS-200033>
- Hamsin, M. K., Halim, A., Anggriawan, R., & Lutfiani, H. (2023). Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection. *Al-Manahij: Jurnal Kajian Hukum Islam*, 17(1), 53–68. <https://doi.org/10.24090/mnh.v17i1.7633>
- IADI. (2021). Core Principles for Effective Banking. *Islamic Financial Services Board*, 1(1–81).
- IMF. (2018). The Core Principles for Islamic Finance Regulations and Assessment Methodology. *Policy Papers*, 18(028), 1. <https://doi.org/10.5089/9781498308496.007>
- Isah Shehu, M., Muhammad Fuad Bin Othman, A., & Binti Osman, N. (2018). The Social Media and Islam. *Sahel Analyst*, 15(4), 67–80.
- Jang, W., & Newman, A. L. (2022). Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation*. *Journal of Common Market Studies*, 60(2), 283–300. <https://doi.org/10.1111/jcms.13215>

- Jankovic, S. D., & Curovic, D. M. (2023). Strategic Integration of Artificial Intelligence for Sustainable Businesses: Implications for Data Management and Human User Engagement in the Digital Era. *Sustainability*, 15(21), 15208. <https://doi.org/10.3390/su152115208>
- Jawi, Z. M., Isa, M. H. M., Solah, M. S., Ariffin, A. H., Shabadin, A., & Osman, M. R. (2016). The future of end-of-life vehicles (elv) in Malaysia - A feasibility study among car users in Klang valley. *MATEC Web of Conferences*, 90. <https://doi.org/10.1051/MATECCONF/20179001038>
- Kaufman, S. (2022). the Invisible, Yet Omnipresent Ear: the Insufficiencies of the Children'S Online Privacy Protection Act. *NYU Annual Survey of American Law*, 78, 101–137. <https://www.oecd-ilibrary.org/sites/71b7058a-en/index.html?>
- Kaul, R. (2019). A Contemporary Analysis of Online Privacy & Data Protection in the context of Parallel Privacy Policies. *Scholedge International Journal of Management & Development*, 6(5), 67–70. <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=bsu&AN=138064047&site=ehost-live&scope=site&custid=s6390179>
- Kaur, J., Dara, R. A., Obimbo, C., Song, F., & Menard, K. (2018). A comprehensive keyword analysis of online privacy policies. *Information Security Journal*, 27(5–6), 260–275. <https://doi.org/10.1080/19393555.2019.1606368>
- Khan, M. I., Haleem, A., & Khan, S. (2018). Defining Halal Supply Chain Management. *Supply Chain Forum*, 19(2), 122–131. <https://doi.org/10.1080/16258312.2018.1476776>
- Kim, W., Park, Y., Shin, J., & Jo, M. (2022). Consumer preference structure of online privacy concerns in an IoT environment. *International Journal of Market Research*, 64(5), 630–651. <https://doi.org/10.1177/14707853221080067>
- Kovalenko, Y. (2022). the Right To Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights. *Masaryk University Journal of Law and Technology*, 16(1), 37–57. <https://doi.org/10.5817/MUJLT2022-1-2>
- Koziol-McLain, J., Vandal, A. C., Wilson, D., Nada-Raja, S., Dobbs, T., McLean, C., Sisk, R., Eden, K. B., & Glass, N. E. (2018). Efficacy of a web-based safety decision aid for women experiencing intimate partner violence: Randomized controlled trial. *Journal of Medical Internet Research*, 20(1). <https://doi.org/10.2196/jmir.8617>
- Light, T. (2021). Data Privacy: One Universal Regulation Eliminating the Many States of Legal Uncertainty. *St. Louis University Law Journal*, 65(4), 873–896.
- Lubis, M., & Kartiwi, M. (2013). Privacy and trust in the Islamic perspective: Implication of the digital age. *2013 5th International Conference on*

- Information and Communication Technology for the Muslim World, ICT4M 2013, IEEE*(August), 1–7. <https://doi.org/10.1109/ICT4M.2013.6518898>
- Masur, P. K., & Trepte, S. (2021). Transformative or Not? How Privacy Violation Experiences Influence Online Privacy Concerns and Online Information Disclosure. *Human Communication Research*, 47(1), 49–74. <https://doi.org/10.1093/hcr/hqaa012>
- Mohamed, A., & Zeki, A. (2023). The Use of Social Network Sites for Healthcare in Islamic Perspective. *Journal of Science and Technology*, 28(1), 24–29. <https://doi.org/10.20428/jst.v28i1.2033>
- Muhammad, A., & Elesin, J. (2022). *Basic principles of Sharī c ah (Islamic Law) Introduction To* (1st ed., Issue August). Ahmadu Bello University Press Limited. <https://www.researchgate.net/publication/363157293>
- Munawar, H., Naamane, D., Fatmir Mehdi, S., & Kabuye Uthman, S. (2010). Ethics and Fiqh for Everyday Life: An Islamic Perspectives. *International Islamic University Malaysia*, 18(Ungs 2050), 1–14.
- Onifade, A. B., Akinwande, K. A., & Shehu, H. (2019). Information Ethics: Islamic Perspectives on Privacy and Hacking. *Journal of Knowledge & Communication Management*, 9(1), 29. <https://doi.org/10.5958/2277-7946.2019.00004.4>
- Ortega, G. M. (2022). FOLLOWING THE ENTRY INTO FORCE OF THE EUROPEAN UNION REGULATION. *Revista Catalana de Dret Public*, 64, 158–173.
- Osman, A. (2023). The Right to be Forgotten: an Islamic Perspective. *Human Rights Review*, 24(1), 53–73. <https://doi.org/10.1007/s12142-022-00672-2>
- Pendaroska, L. (2021). International Transfer of Personal Data between the EU and Countries outside the EU. *Iustianus Primus Law Review*, 1–13.
- Petit, P. (2020). ‘Everywhere Surveillance’: Global Surveillance Regimes as Techno-Securitization. *Science as Culture*, 29(1), 30–56. <https://doi.org/10.1080/09505431.2019.1586866>
- Radi, S. M. (2022). The right to the protection of personal data under the Constitution of the Republic of Iraq for the Year 2005. *Imam Ja’afar Al-Sadiq University of Legal Studies*, 1(4), 147–171. <https://www.iasj.net/iasj/issue/15313>
- Romansky, R. P. (2022). Digital Age and Personal Data Protection. *International Journal on Information Technologies & Security*, 14(3), 89–100. <https://www.researchgate.net/publication/362695987>
- Sahih al-Bukhari. (6066). *Hadith on Good Manners and Firm (Al-Adab)*. Book 78. <https://www.isamicity.org/hadith/search/index.php?q=5825&sss=1>
- Saputra, A. A., Fasa, M. I., & Ambarwati, D. (2022). Islamic-Based Digital Ethics:

- The Phenomenon of Online Consumer Data Security. *Share: Jurnal Ekonomi Dan Keuangan Islam*, 11(1), 105. <https://doi.org/10.22373/share.v11i1.11167>
- Sherwani, M. (2018). The Right to Privacy under International Law and Islamic Law: A Comparative Legal Analysis. *Kardan Journal of Social Sciences and Humanities*, 1(1), 30–48. <https://doi.org/10.31841/kjssh.2021.14>
- Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: a case of saudi arabia. *Beijing Law Review*, 11(3), 637–650.
- Skowronski, D. S. (2022). COPPA and Educational Technologies: The Need for Additional Online Privacy Protections for Students. *Georgia State University Law Review*, 38(4), 1217–1252. <https://www.who.int/news-room/fact-sheets/detail/autism-spectrum-disorders>
- Škrinjarić, B., Budak, J., & Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. *Economic Research-Ekonomska Istrazivanja*, 32(1), 982–1000. <https://doi.org/10.1080/1331677X.2019.1585272>
- Teo, S. A. (2023). Human dignity and AI: mapping the contours and utility of human dignity in addressing challenges presented by AI. In *Law, Innovation and Technology* (Vol. 15, Issue 1). <https://doi.org/10.1080/17579961.2023.2184132>
- Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. (2016). *Public-Private Cybersecurity*. 41–97. https://doi.org/10.1007/978-1-4471-5216-3_2
- Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research*, 20(3), 565–587. <https://doi.org/10.1007/s10660-020-09422-3>
- Whaiduzzaman, M., Barros, A., Chanda, M., Barman, S., Sultana, T., Rahman, M. S., Roy, S., & Fidge, C. (2022). A Review of Emerging Technologies for IoT-Based Smart Cities. *Sensors*, 22(23), 1–29. <https://doi.org/10.3390/s22239271>
- Younies, H., & el Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, 27(4), 1089–1105.
- Zhang, N., Wang, C., Karahanna, E., & Xu, Y. (2022). Peer Privacy Concern: Conceptualization and Measurement. *MIS Quarterly: Management Information Systems*, 46(1), 491–530. <https://doi.org/10.25300/MISQ/2022/14861>